UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,922	04/12/2001	Gregory O'Shea	171135.01	3840

22971 7590 02/27/2006

MICROSOFT CORPORATION
ATTN: PATENT GROUP DOCKETING DEPARTMENT
ONE MICROSOFT WAY
REDMOND, WA 98052-6399

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 02/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/833,922	O'SHEA ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5-13 and 16-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5-13 and 16-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on January 19, 2006. Claims 1, 2, 5 – 13 and 16 – 25 are pending.

Response to Arguments

2. Applicant's remarks/arguments filed on January 19, 2006, with respect to Claims 1 – 17, 21 and 22, have been fully considered but they are not persuasive.

3. Regarding Claims 1, 2, 5 – 13 and 16 – 25, Applicant argues that O'SHEA et al. (Child-proof Authentication for MIPV6 ACM) is not prior art since it was not published more than one year prior to the application date November 13, 2001. Examiner points out that the Information Disclosure Statement (IDS) filed on 4/14/2003 with the instant application, discloses "Child-proof authentication for MIPV6", 5 pages discloses the earliest publication date of Month 1-2, 2000 (Copyright 2000 ACM 1-58113), which is more than one year before the instant application date (April 12, 2001).

Applicant clearly has failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. Therefore, the examiner respectfully asserts that cited prior art does teach or suggest the subject matter broadly recited in Claims 1, 2, 5 – 13 and 16 – 25.

Accordingly, the 35 USC 103 rejection for the pending Claims 1, 2, 5 – 13 and 16 – 25 is respectfully maintained.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1, 2, 5 – 13 and 16 – 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Diffie et al (U.S. Patent Number Re. 36,946, hereafter "Diffie") in view of Greg O'Shea (ACM 2000, hereafter "Greg").

5. Regarding Claims 1 and 12, Diffie teaches and describes

creating authentication information, the authentication information including content data that include data fro updating a care-of address of the mobile computing device (Diffie Column 5 line 34 – Column 6 line 18 and Column 8 lines 18 – 64),

Diffie teaches that the content data include data for updating a public key of the device (digital signature with the public key and the machine name (care-of address)), a public key of the first computing device, and a digital signature, the digital signature generated by signing with a private key of the mobile computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data (Fig. 4a – 4c, 5a; and Column 1 line 49 –

Column 2 line 20 and Column 7 lines 6 – 45); and making the authentication information available to the second computing device.

Diffie does not explicitly teach that the authentication information includes a network address of the mobile computing device, the network address having a portion derived from the public key of the mobile computing device. However, Greg discloses a unilateral authentication protocol wherein a network address of a mobile node (computing device) is derived from the public key of the mobile computing device (Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and "Integrating CAM into MIPV6").

6. Motivation to combine the invention of Diffie with O'Shea's teachings comes from the need for secure transaction and authentication of mobile devices with the base device. Diffie et al. themselves provide a discussion of the need for authentication security but are silent as to the specific details of the technical network address manipulation involved, see Diffie Column 4 line 10 – Column 5 line 33 and Column 6 line 60 – Column 8 line 67. It would have been obvious to one of ordinary skill in the art to combine Diffie et al with O'Shea because security and device authentication is needed for mobile devices of Diffie and O'Shea provides some details of how to authenticate and secure mobile device communications with the base device. O'Shea could have been modified by Diffie because Diffie provides a secure communication link between a mobile wireless data processing device and a base data processing device

and O'Shea discloses a specialized security system for unilateral authentication protocol.

7. Regarding Claim 13, Diffie teaches and describes

content data that include data for updating a care-of address of a computing device (Diffie Column 5 line 34 – Column 6 line 18 and Column 8 lines 18 – 64),

Diffie teaches that the content data include data for updating a public key of the device (digital signature with the public key and the machine name (care-of address)),

a public key of the computing device; and a digital signature, the digital signature generated by signing with a private key of the computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data (Fig. 4a – 4c, 5a; and Diffie Column 1 line 49 – Column 2 line 20 and Column 7 lines 6 – 45).

Diffie does not explicitly teach that the authentication information includes a network address of the computing device, the network address having a portion derived from the public key of the computing device. However, Greg discloses a unilateral authentication protocol wherein a network address of a node (computing device) is derived from the public key of the computing device (Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and "Integrating CAM into MIPV6").

8. Motivation to combine the invention of Diffie with O'Shea's teachings comes from the need for secure transaction and authentication of mobile devices with the base

device. Diffie et al. themselves provide a discussion of the need for authentication security but are silent as to the specific details of the technical network address manipulation involved, see Diffie Column 4 line 10 – Diffie Column 5 line 33 and Diffie Column 6 line 60 – Diffie Column 8 line 67. It would have been obvious to one of ordinary skill in the art to combine Diffie et al with O'Shea because security and device authentication is needed for mobile devices of Diffie and O'Shea provides some details of how to authenticate and secure mobile device communications with the base device. O'Shea could have been modified by Diffie because Diffie provides a secure communication link between a mobile wireless data processing device and a base data processing device and O'Shea discloses a specialized security system for unilateral authentication protocol.

9. Regarding Claims 20 and 25, Diffie teaches and describes

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature; validating the digital signature by using the public key of the first computing device; accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data (Fig. 4a – 4c, 5a, 5b; and Diffie Column 1 line 49 – Column 2 line 20 and Column 7 line 46 – Column 8 line 58).

Diffie does not explicitly teach deriving a portion of a second network address from the public key of the first computing device. However, Greg discloses a unilateral authentication protocol wherein a network address of a mobile node (computing device) is derived from the public key of the mobile computing device (Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and "Integrating CAM into MIPV6").

10. Motivation to combine the invention of Diffie with O'Shea's teachings comes from the need for secure transaction and authentication of mobile devices with the base device. Diffie et al. themselves provide a discussion of the need for authentication security but are silent as to the specific details of the technical network address manipulation involved, see Diffie Column 4 line 10 – Column 5 line 33 and Column 6 line 60 – Column 8 line 67. It would have been obvious to one of ordinary skill in the art to combine Diffie et al with O'Shea because security and device authentication is needed for mobile devices of Diffie and O'Shea provides some details of how to authenticate and secure mobile device communications with the base device. O'Shea could have been modified by Diffie because Diffie provides a secure communication link between a mobile wireless data processing device and a base data processing device and O'Shea discloses a specialized security system for unilateral authentication protocol.

11. Claim 2 is rejected as applied about in rejecting Claim 1. Furthermore, Diffie discloses wherein the authentication information is made available to the base

computing device by sending a message incorporating the authentication information to the base computing device (Diffie Column 7 lines 38 – 45).

12. Claim 5 is rejected as applied about in rejecting Claim 1 and 13. Furthermore, Diffie discloses wherein the second computing device is a home agent for the mobile computing device, and wherein the network address of the mobile computing device is a home address of the mobile computing device (Diffie Column 7 lines 6 – 10 and Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and "Integrating CAM into MIPV6").

13. Claims 6 and 16 are rejected as applied about in rejecting Claim 1. Furthermore, Diffie discloses wherein the base computing device is a correspondent of the mobile computing device, and wherein the network address of the mobile computing device is a home address of the mobile computing device (Diffie Column 7 lines 6 – 10 and Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and "Integrating CAM into MIPV6").

14. Claim 7 is rejected as applied about in rejecting Claim 1. Furthermore, Diffie discloses wherein the public key and the private key together form an uncertified key pair (Diffie Column 5 line 51 – Column 6 line 7).

15. Claims 8 and 17 are rejected as applied about in rejecting Claims 1 and 13. Furthermore, Diffie discloses wherein the network address of the mobile computing device includes a route prefix portion and a node-selectable portion, and the node-selectable portion includes a portion of a hash value of data including the public key of the mobile computing device (Diffie Column 7 lines 6 – 29 and Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and "Integrating CAM into MIPV6").

16. Claims 10 and 19 are rejected as applied about in rejecting Claims 1 and 13. Furthermore, Diffie discloses wherein the authentication information further includes data for preventing a replay attack (Diffie Column 8 lines 12 – 58 and Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and "Integrating CAM into MIPV6").

17. Claim 21 is rejected as applied about in rejecting Claim 20. Furthermore, Diffie discloses determining whether to accept the content data based on a time stamp in the authentication information (Diffie Column 7 lines 6 – 10 and Column 8 lines 18 – 32 and Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and "Integrating CAM into MIPV6").

18. Claims 9 and 18 are rejected as applied about in rejecting Claims 8 and 17. Furthermore, Diffie discloses wherein the node-selectable portion includes a portion of a hash value of data including the public key of the mobile computing device and a modifier selected for preventing address conflicts (Diffie Column 7 lines 23 – 45 and

Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and "Integrating CAM into MIPV6").

19. Claim 11 is rejected as applied about in rejecting Claim 10. Furthermore, Diffie discloses wherein the data for preventing a replay attack are in the set: time stamp, data identifying the second computing device as an intended recipient of the authentication information (Diffie Column 7 lines 6 – 45 and Column 8 lines 49 – 58 and Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and "Integrating CAM into MIPV6").

20. Claim 22 is rejected as applied about in rejecting Claim 20. Furthermore, Diffie discloses wherein the content data include data for updating a communications parameter for the first computing device, the method further comprising updating a record of a communications parameter for the first computing device (Diffie Column 7 line 38 – Column 8 line 67).

21. Claim 24 is rejected as applied about in rejecting Claim 20. Furthermore, Diffie discloses wherein the authentication information further includes a modifier, and wherein deriving includes appending the modifier to the public key of the first computing device before deriving a portion of the second network address (Diffie Column 8 lines 7 – 68 and Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and "Integrating CAM into MIPV6").

22. Claim 23 is rejected as applied about in rejecting Claim 22. Furthermore, Diffie discloses wherein the communications parameter is a care-of address of the first computing device, and wherein updating includes updating a routing table maintained by the second computing device (Diffie Column 8 lines 7 – 68 and Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and "Integrating CAM into MIPV6").

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are

applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
February 18, 2006.

CPP
Primary Examiner
AU 2131
2/20/06